enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

DE

Von Januar 2019 bis April 2020

Schadprogramme (Malware)

ENISA Threat Landscape

Überblick

Malware ist eine häufige Art von Cyberangriffen in Form von schädlicher Software. Zu den Familien von Malware gehören Kryptominierer, Viren, Ransomware, Würmer und Spyware. Ihre gemeinsamen Ziele sind Informations- oder Identitätsdiebstahl, Spionage und Betriebsstörungen.[1]

Im Jahr 2019 waren Kryptominierer eine der am weitesten verbreiteten Malware-Familien in der Bedrohungslandschaft,[2], was zu hohen IT-Kosten, einem erhöhten Stromverbrauch und einer verringerten Mitarbeiterproduktion führte.[3] Ransomware verzeichnete 2019 einen leichten Anstieg gegenüber 2018, blieb jedoch weiterhin ganz unten auf der Malware-Typliste.[2]

Web- und E-Mail-Protokolle waren die häufigsten anfänglichen Angriffsmethoden, mit denen Malware verbreitet wurde. Mithilfe von Brute-Force-Techniken oder der Ausnutzung von Systemschwachstellen konnten sich bestimmte Malware-Familien jedoch innerhalb eines Netzwerks noch weiter verbreiten. Obwohl die weltweiten Entdeckungen von Angriffen auf dem Niveau des Vorjahres geblieben sind, gab es eine spürbare Verschiebung von Verbraucher- zu Geschäftszielen.[4]

Erkenntnisse

400.000 Entdeckungen von vorinstallierter Spyware und Adware auf Mobilgeräten[4]

13 % Zunahme der Windows-Malware-Erkennung an Geschäftsendpunkten[4]

71 % der Unternehmen erkannten Malware-Aktivitäten, die sich von einem Mitarbeiter auf einen anderen ausbreiteten[47]

46,5 % aller Malware in E-Mail-Berichten wurden im Dateityp „docx“ gefunden[24]

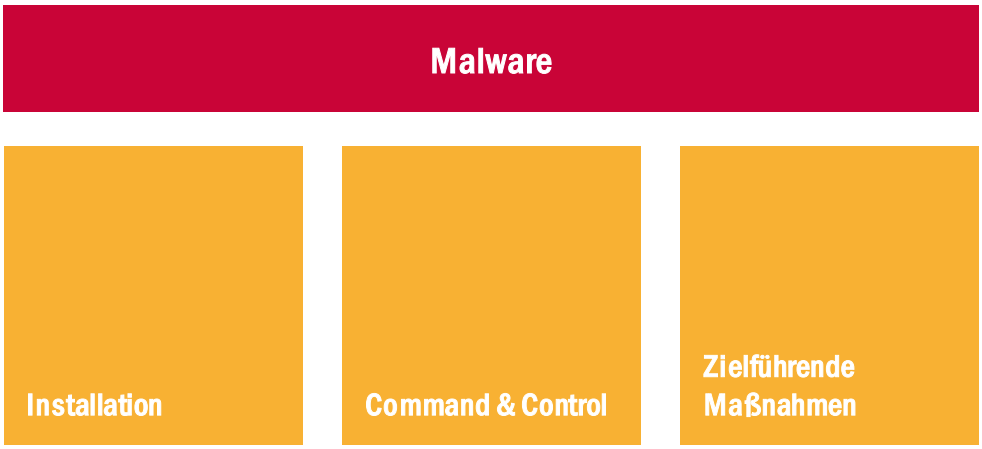
50 % Zunahme von Malware zum Diebstahl persönlicher Daten oder Stalkerware[15]

67 % der Malware wurden über verschlüsselte HTTPS-Verbindungen bereitgestellt[48]

Kill chain

Schritt des Angriffs-Workflows

Umfang des Zwecks



Das Cyber Kill Chain® Framework wurde von Lockheed Martin entwickelt und basiert auf einem militärischen Konzept, das mit der Struktur eines Angriffs zusammenhängt. Um einen bestimmten Angriffsvektor zu untersuchen, verwenden Sie dieses Kill-Chain-Diagramm, um jeden Schritt des Prozesses sowie die vom Angreifer verwendeten Hilfsmittel, Techniken und Verfahren festzuhalten.

WEITERE INFORMATIONEN

Die am häufigsten verwendeten Malware-Typen

Emotet war 2019 die am weitesten verbreitete Malware und entwickelte sich 2020 weiter. Emotet wurde ursprünglich 2014 als Bankentrojaner entdeckt. Seitdem wurde es mit Befehls- und Steuerungsfunktionen (C2), zusätzlichen Ausweichmechanismen wie der Fähigkeit, festzustellen, ob es in einer Sandbox-Umgebung ausgeführt wird, und der Fähigkeit, gefährliche Payloads wie Trickbot und Ryuk zu liefern, aktualisiert.[7] Die obige Abbildung zeigt das im Jahr 2019 festgestellte Ranking von Banking-Malware.

Im Berichtszeitraum entwickelte sich Emotet zu einem Botnetz[2], erhöhte seine Aktivität[8] und initiierte neue lokalisierte Spam-Kampagnen mit Spear-Phishing-Funktionen, um Ransomware zu installieren oder Informationen zu stehlen.[5] Im Jahr 2019 stiegen die Erkennungen von Emotet im Vergleich zum Vorjahr um 73 %, hauptsächlich für Unternehmenziele in den USA und im Vereinigten Königreich, wie in der folgenden Abbildung dargestellt.[4]

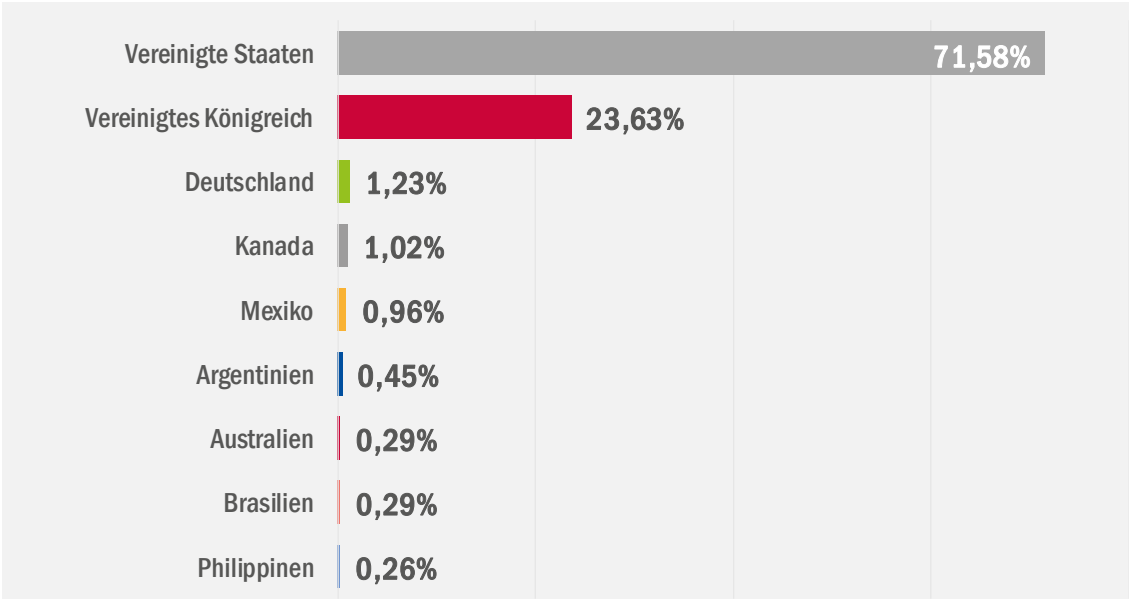


Abbildung 1: 2019 weltweite Emotet-Erkennungen nach Ländern. Quelle MalwareBytes[4]

_Eine Verschiebung in Richtung Geschäftsziele

Obwohl die Malware-Erkennung weltweit auf dem Niveau von 2018 blieb[4,9], wurde in den am stärksten betroffenen Sektoren ein Anstieg der Malware-Zielunternehmen in den Bereichen Dienstleistungen, Bildung und Einzelhandel um 13 % beobachtet.[4] Schätzungen zufolge richteten sich mehr als ein Drittel der Banking-Malware-Angriffe im Jahr 2019 an gewerbliche Benutzer mit der Absicht, die finanziellen Ressourcen des Unternehmens zu gefährden.[10] Die fünf wichtigsten Arten von Malware[4], die auf Unternehmen abzielen, waren Trojan.Emotet, Adware.InstallCore, HackTool.WinActivator, Riskware.BitCoinMiner und Virus.Renamer. Ransomware-Angriffe gegen den öffentlichen Sektor nahmen 2019 zu, da hier höhere Lösegeldzahlungen möglich waren.[11] Da Cyberkriminelle hochwertige Ziele anstreben, wurden neue Malware-Typen so konzipiert, dass sie sich seitlich innerhalb eines Unternehmensnetzwerks und nicht über das Internet verbreiten.[12]

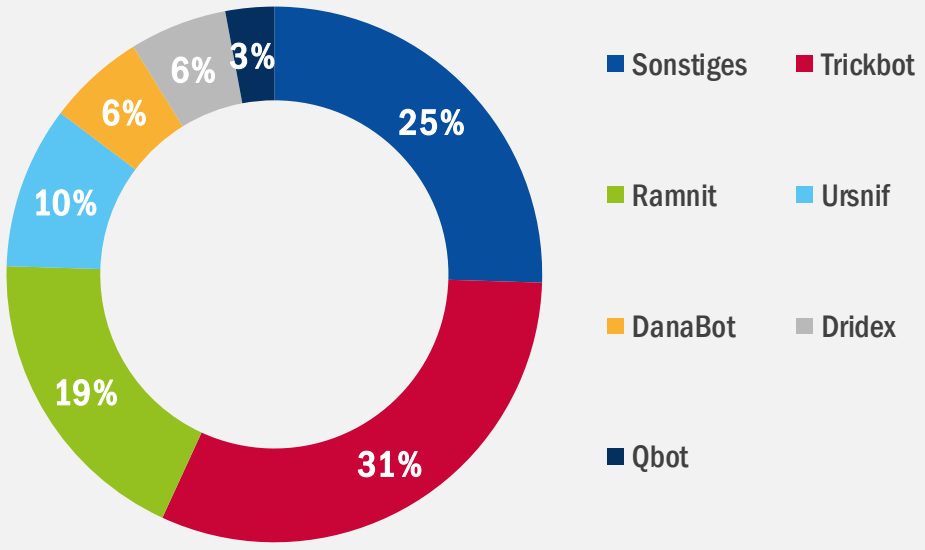


Abbildung 2: Weltweite Banking-Malware Erkennungen in 2019. Quelle: CheckPoint[2]

Entwicklungen

_ Malware-as-a-Service (MaaS)

Malware-as-a-Service (MaaS) bezeichnet eine bestimmte Malware, die in Untergrund-Foren verkauft wird und Kunden (Cyberkriminellen) die für gezielte Angriffe erforderlichen Instrumente und Infrastrukturen zur Verfügung stellt. Ein MaaS-Besitzer bietet diesen Service durch die Lieferung eines Kits an, das einen Erstlader, einen Befehls- und Steuerungsserver (C2) und eine Hintertür zur vollständigen Kontrolle über den infizierten Computer enthält.

Ein Sicherheitsforscher[13] identifizierte kürzlich vier Arten von Angriffen mit verschiedenen Tools aus dem Malware-as-a-Service-Portfolio (MaaS) von Golden Chickens (GC) und bestätigte die Veröffentlichung verbesserter Varianten mit Code-Updates für drei dieser Instrumente.

- **TerraLoader**. Ein in PureBasic geschriebener Mehrzwecklader. TerraLoader ist ein Flaggschiff des GC MaaS-Serviceportfolios.
- **more_eggs**. Eine Backdoor-Malware, die in der Lage ist, auf einen festen C2-Server zu übertragen und zusätzliche Payloads auszuführen, die von einer externen Webressource heruntergeladen wurden. Die Hintertür ist in JavaScript geschrieben.
- **VenomLNK**. Eine Windows-Verknüpfungsdatei, die wahrscheinlich von einer neueren Version des VenomKit-Baukastens generiert wurde.

Mobile Banking-Malware im Aufmarsch

Mobile Anwendungen zum Stehlen von Zahlungsdaten, Anmeldedaten und Geldern von den Bankkonten der Opfer stiegen im ersten Halbjahr 2019 um 50 %.[14] Traditionell haben Bedrohungsakteure Phishing-Techniken verwendet, um Bankanmeldedaten zu erhalten, indem sie entweder eine gefälschte Seite anzeigen, die den Login der Bank nachahmt oder durch Einführung gefälschter mobiler Apps, die den Original-Banking-Apps ähneln. Im Jahr 2019 wurden Cyberkriminelle jedoch kreativer, wie im Fall von Trojan-Banker.AndroidOS.Gustuff.a, das in der Lage war, eine legitime Banking-App durch Missbrauch der Eingabehilfen des Betriebssystems zu steuern und dadurch böswillige Transaktionen zu automatisieren.[15] Neue Versionen mobiler Finanz-Malware wurden häufig in Untergrundforen zum Verkauf gefunden[15,] und es wurden kontinuierlich neue Ausweichtechniken entwickelt. Eine bemerkenswerte Neuerung, die 2019 entdeckt wurde, war die Fähigkeit von Malware, Bewegungssensoren zu verwenden und nur ausgelöst zu werden, wenn sich ein Smartphone bewegt, wie es der Mobile-Banking-Trojaner Annubis verwendet, um eine Sandbox-Umgebung zu erkennen.[16] Die beliebteste Banking-Malware in 2019[11] war Asacub (44,4 %), Svpeng (22,4 %), Agent (19,1 %), Faketoken (12 %) und Hqwar (3,8 %).

Entwicklungen

_Dateifreie Malware

Dateifreie Malware enthält keine ausführbare Datei und kann gängigen Sicherheitsfiltern und Whitelist-Techniken entgehen. Aus diesem Grund kann es bis zu zehnmal wahrscheinlicher sein, dass diese Malware-Familie erfolgreicher ist als die anderen.[18] Anstelle einer ausführbaren Datei muss der Angreifer bei dieser Art von Malware einen bösartigen Code in bereits installierte und vertrauenswürdige Software einfügen, entweder auf Abstand (z. B. im Fall von Windows Management Instrumentation oder WMI und PowerShell) oder durch aktives Herunterladen von Dokumentdateien (z. B. Office-Dokumenten), die schädliche Makros enthalten.[19] Nach einem erfolgreichen Angriff kann die Malware über die Registrierung, den integrierten Taskplaner oder das WMI an Persistenz gewinnen. Dateifreie Malware-Angriffe nahmen im ersten Halbjahr 2019 um 265 % zu.[20] Die meisten dieser Angriffe waren skriptbasiert (38 %), während andere einen In-Memory-Angriff ausführten (24 %) oder integrierte Systemtools missbrauchten (20 %).[21]

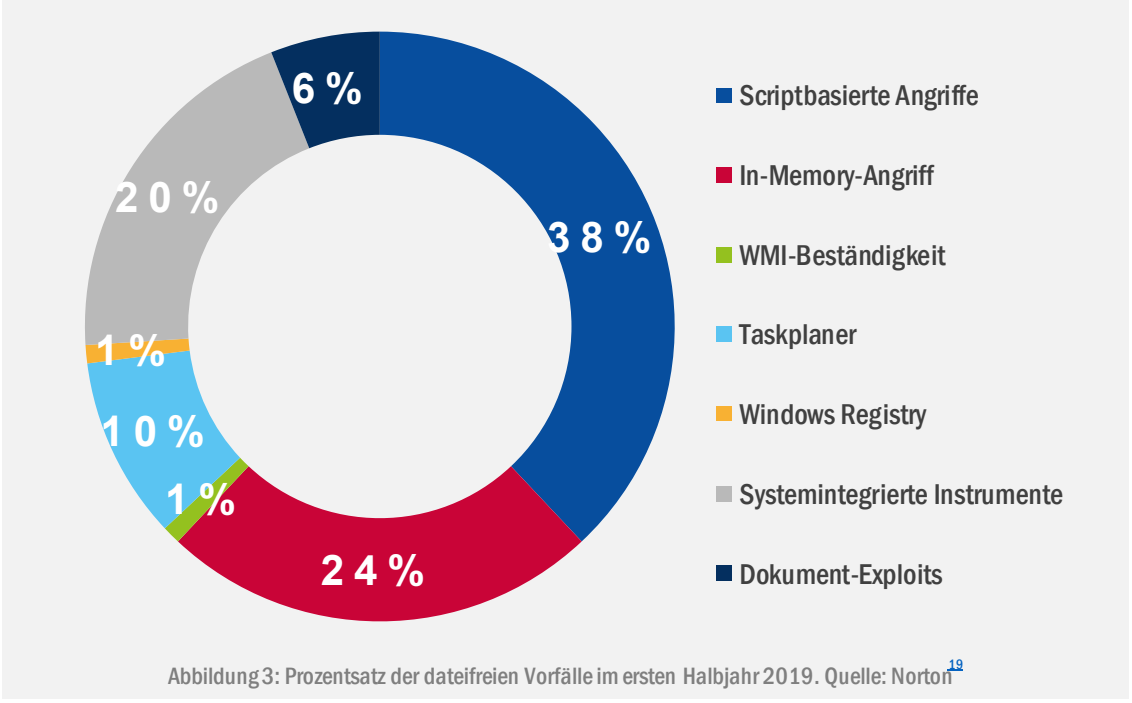


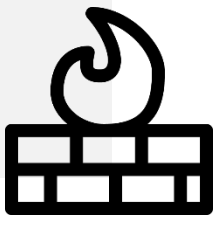
Abbildung 3: Prozentsatz der dateifreien Vorfälle im ersten Halbjahr 2019. Quelle: Norton[19]

Wie kann man einem dateifreien Angriff vorbeugen und diesen abwehren?

Der effektivste Weg für Unternehmen, sich gegen dateifreie Angriffe zu verteidigen, besteht darin, die Software auf dem neuesten Stand zu halten. Da die meisten dateifreien Infektionen bei Microsoft-Anwendungen und insbesondere bei DOCX-Dateien auftreten, ist es besonders wichtig, diese Software ständig auf die neueste Version zu aktualisieren. Microsoft hat außerdem sein Windows Defender-Paket aktualisiert, um unregelmäßige Aktivitäten mithilfe der PowerShell-Anwendung zu erkennen.

Laut einem Sicherheitsforscher[18] besteht der Schlüssel zur erfolgreichen Bekämpfung einer dateifreien Angriffskampagne darin, jede Phase des Lebenszyklus der Bedrohung mit einem integrierten und vielschichtigen Verteidigungsansatz zu bewältigen. Bei diesem Ansatz ist es wichtig, die verschiedenen Phasen des Angriffs zu untersuchen und die folgenden Aktivitäten durchzuführen:

- Analyse und Messung der vom Angreifer ausgeführten Aktionen;
- Identifizierung der verwendeten Techniken;
- Überwachung von Aktivitäten in PowerShell oder anderen Scripting-Engines;
- Zugang zu aggregierten Bedrohungsdaten;
- Kontrolle des Zustands des Zielsystems;
- Stoppen willkürlicher Prozesse;
- Korrektur von Prozessen, die Teil des Angriffs sind;
- Isolierung infizierter Geräte.



Entwicklungen

_Botnetz- und Command and Control (C&C)-Landschaft

Der weltweite Botnetz-Verkehr stieg seit 2018 um 71,5 % an[2]. Die am häufigsten beobachteten Botnetze waren Emotet (41 %), Trickbot (25 %) und DanaBot (5 %)[2]. In Russland war ein deutlicher Anstieg des Botnetz-Verkehrs zu beobachten (143 %), der hauptsächlich auf lockere Registrierungsverfahren und ein geringeres Interesse der Strafverfolgungsbehörden zurückzuführen war.[14] Im Jahr 2019 waren in Russland die meisten Botnetz-C2s angesiedelt, gefolgt von den USA, den Niederlanden, China und Frankreich. Algorithmen zur Generierung von Domainnamen (DGAs) wurden von Cyberkriminellen verwendet, um viele C2-Kommunikationen zu unterstützen. 50 % dieser Registrierungen erfolgten in Top-Level-Domains (TLDs) „.com“ und „.net“.[15] Im Berichtszeitraum gingen diese Registrierungen von Domainnamen um 71 % zugunsten anderer Kommunikationsprotokolle wie Peer-to-Peer (P2P) zurück.[13]

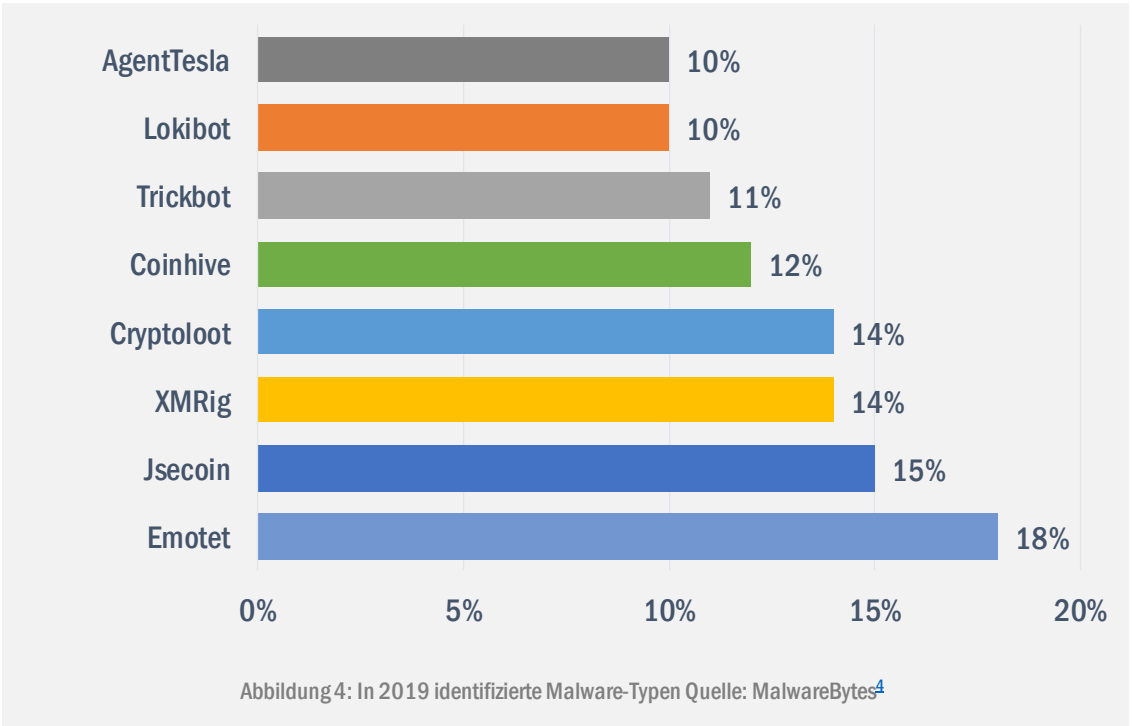


Abbildung 4: In 2019 identifizierte Malware-Typen Quelle: MalwareBytes[4]

_Wie

Laut einer Studie aus dem Jahr 2019 wurden 94 % aller Malware-Typen per E-Mail übermittelt.[24] Obwohl dies als Einstiegspunktvektor gezählt wird, ist es interessant festzustellen, dass bei einem erfolgreichen Angriff die Malware möglicherweise eine zusätzliche Payload herunterlädt, die ein wurmartiges Verhalten zeigt, um eine seitliche Ausbreitung im Netzwerk zu ermöglichen (Emotet und Trickbot). Darüber hinaus verbreitete sich Malware nach der erstmaligen Bereitstellung in den meisten Fällen (71 %) durch die Aktivitäten der Mitarbeiter. Erneut erregten neue Sicherheitslücken im Remotedesktopprotokoll (RDP) Aufmerksamkeit, da sie die Remotecodeausführung (RCE) ermöglichen und daher wurmfähig sind.[30] Obwohl diese neu entdeckten Sicherheitslücken nicht in großem Umfang ausgenutzt wurden, wird erwartet, dass ein neuer Wurm in naher Zukunft auf nicht gepatchte Systeme abzielen könnte.[31]

_Vorfälle

- **Airbus** erlitt eine Datenschutzverletzung, die Mitarbeiter in Europa betraf.[34,35]
- Malware zum Skimmen von Karten, die auf der Website der **American Medical Collection Agency** installiert wurde, führte zum Diebstahl der personenbezogenen Daten von 12 Millionen Patienten.[36]
- Der größte Anbieter von Labordiagnostik **LifeLabs** wurde Opfer eines Ransomware-Angriffs, der zum Diebstahl von 15 Millionen Konten mit Testergebnissen und Gesundheitskartennummern führte.[37,38]
- Ein Ransomware-Angriff auf die **Stadt Pensacola, Florida,** führte dazu, dass 2 GB Daten online verfügbar gemacht wurden, die möglicherweise personenbezogene Daten (PII) enthielten.[39]
- Die personenbezogenen Daten von 2.400 Mitarbeitern der Streitkräfte in Singapur wurden möglicherweise durch E-Mail-Phishing durch bösartige Malware entwendet.[40]

Minderung

_ Vorgeschlagene Maßnahmen

- Implementieren Sie die Malware-Erkennung für alle eingehenden/ausgehenden Kanäle, einschließlich E-Mail-, Netzwerk-, Web- und Anwendungssysteme, auf allen anwendbaren Plattformen (d. h. Servern, Netzwerkinfrastruktur, PCs und Mobilgeräten).
- Überprüfen Sie den SSL/TLS-Verkehr, damit die Firewall entschlüsseln kann, was an und von Websites, E-Mail-Kommunikation und mobilen Anwendungen übertragen wird.
- Richten Sie Schnittstellen zwischen Malware-Erkennungsfunktionen (nachrichtendienstliche Bedrohungssuche) und Sicherheitsvorfallmanagement ein, um effiziente Reaktionsfunktionen einzurichten.
- Verwenden Sie die für die Malware-Analyse verfügbaren Instrumente zum Austausch von Malware-Informationen und zur Minderung von Malware (z. B. MISP).[32]
- Entwickeln Sie Sicherheitsrichtlinien, die die Prozesse angeben, die im Falle einer Infektion einzuhalten sind.
- Verstehen Sie die Funktionen verschiedener Sicherheitstools und entwickeln Sie neue Sicherheitslösungen. Identifizieren Sie Lücken und wenden Sie das Prinzip der Tiefenverteidigung an.
- Verwenden Sie die E-Mail-Filterung (oder Spam-Filterung) für böswillige E-Mails und entfernen Sie ausführbare Anhänge.
- Überwachen Sie regelmäßig die Ergebnisse von Antivirentests.[30,42]
- Protokollüberwachung mit der SIEM-Lösung (Security Incident and Event Management). Indikative Protokollquellen sind Antiviren-Warnungen, Endpoint Detection and Response (EDR), Proxyserver-Protokolle, Windows Event- und Sysmon[43] Protokolle, IDS-Protokolle (Intrusion Detection System)[44], usw.
- Deaktivieren oder reduzieren Sie den Zugriff auf PowerShell-Funktionen.[45]

"Die Komplexität der Bedrohungsfähigkeiten nahm 2019 zu, und viele Gegner nutzten Exploits, Diebstahl von Anmeldeinformationen und mehrstufige Angriffe."

In ETL 2020

Literaturangaben

1. "What is Malware". Veracode. https://www.veracode.com/security/malware

2. "Cyber Security Report". 2019. Checkpoint. https://www.checkpoint.com/downloads/resources/cyber-security-report-2020.pdf

3. "Beapy: Cryptojacking Worm Hits Enterprises in China" 24. April, 2019. Broadcom. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/beapy-cryptojacking-worm-china

4. "2020 State of Malware Report". Februar 2020 Malware Bytes. https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf

5. "Evasive Threats, Pervasive Effects" 2019. Trend Micro, Research. https://documents.trendmicro.com/assets/rpt/rpt-evasive-threats-pervasive-effects.pdf

6 "SonicWall Cyber Threat Report". 2020. SonicWall. https://www.sonicwall.com/resources/2020-cyber-threat-report-pdf/

7. "Emotet is back: botnet springs back to life with new spam campaign". 16. September, 2019. Malwarebytes Labs. https://blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign/

8. "Increased Emotet Malware Activity" 22. Januar, 2020. US CERT. https://www.us-cert.gov/ncas/current-activity/2020/01/22/increased-emotet-malware-activity

9. "SonicWall Security Metrics" SonicWall. https://securitycenter.sonicwall.com/m/page/capture-labs-threat-metrics

10. "Over a third of banking malware attacks in 2019 targeted corporate users – demonstrating the need for protection". 16. April, 2019. Kaspersky. https://www.kaspersky.com/about/press-releases/2020_over-a-third-of-banking-malware-attacks-in-2019-targeted-corporate-users-demonstrating-the-need-for-protection

11. "Internet organised crime threat assessment" 2019. EUROPOL (EC3). https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf

12. "Narrowed Sights, Bigger Payoffs: Ransomware in 2019" 6. Juni, 2019. Trend Micro. https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/narrowed-sights-bigger-payoffs-ransomware-in-2019

13. "GOLDEN CHICKENS: Evolution of the MaaS". 20. Juli, 2020. QuoIntelligence. https://quointelligence.eu/2020/07/golden-chickens-evolution-of-the-maas/

14. "From Supply Chain to Email, Mobile and the Cloud" 25. Juli, 2019. CheckPoint. https://www.checkpoint.com/press/2019/check-point-research-from-supply-chain-to-email-mobile-and-the-cloud-no-environment-is-immune-to-cyber-attacks/

15. "Mobile malware evolution 2019". 25. Februar, 2020. Kaspersky. https://securelist.com/mobile-malware-evolution-2019/96280/

16. "Google Play Apps Drop Anubis Banking Malware, Use Motion-based Evasion Tactics". 17. Januar, 2019. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/google-play-apps-drop-anubis-banking-malware-use-motion-based-evasion-tactics/

17. "Spamhaus Botnet Threat Report 2019". 28. Januar, 2020. Spamhaus. https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019

18. "What Is Fileless Malware?". McAfee. https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html

19. "What is fileless malware and how does it work?". Norton. https://us.norton.com/internetsecurity-malware-what-is-fileless-malware.html

20. "Trend Micro Report Reveals 265% Growth In Fileless Events". 28. August, 2019. Trend Micro. https://www.trendmicro.com/en_hk/about/newsroom/press-releases/2019/2019-08-28.html

21. "Understanding Fileless Threats" 29. Juli, 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/security-technology/risks-under-the-radar-understanding-fileless-threats

22. "SonicWall Sees Dramatic Jump In IoT Malware, Encrypted Threats, Web App Attacks Through Third Quarter". 22. Oktober, 2019. SonicWall. https://www.sonicwall.com/news/dramatic-jump-in-iot-malware-encrypted-threats-web-app-attacks-third-quarter/

23. "2020 Vulnerability and Threat Trends". 2020. SKYBOX. https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/2020_VT_Trends-Report-reduced.pdf

24. "Over a third of banking malware attacks in 2019 targeted corporate users – demonstrating the need for protection". 16. April, 2019. Kaspersky. https://www.kaspersky.com/about/press-releases/2020_over-a-third-of-banking-malware-attacks-in-2019-targeted-corporate-users-demonstrating-the-need-for-protection

25. "Internet organised crime threat assessment" 2019. EUROPOL(EC3). https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf

26. "Narrowed Sights, Bigger Payoffs: Ransomware in 2019" 6. Juni, 2019. Trend Micro. https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/narrowed-sights-bigger-payoffs-ransomware-in-2019

27. "From Supply Chain to Email, Mobile and the Cloud" 25. Juli, 2019. CheckPoint. https://www.checkpoint.com/press/2019/check-point-research-from-supply-chain-to-email-mobile-and-the-cloud-no-environment-is-immune-to-cyber-attacks/

28. "Mobile malware evolution 2019". 25. Februar, 2020. Kaspersky. https://securelist.com/mobile-malware-evolution-2019/96280/

29. "Mobile banking malware surges in 2019". 25. Juli, 2019. Computer Weekly. https://www.computerweekly.com/news/252467340/Mobile-banking-malware-surges-in-2019

30. "Google Play Apps Drop Anubis Banking Malware, Use Motion-based Evasion Tactics". 17. Januar, 2019. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/google-play-apps-drop-anubis-banking-malware-use-motion-based-evasion-tactics/

31. "BlueKeep attacks are happening, but it's not a worm". 3. November, 2019. ZDNet. https://www.zdnet.com/article/bluekeep-attacks-are-happening-but-its-not-a-worm/

32. MISP Projects. http://www.misp-project.org/

33. "PowerShell, fileless malware's great attack vector" . 25. Februar, 2019. Panda. https://www.pandasecurity.com/mediacenter/malware/powershell-fileless-malware-attack-vector/

34. "Airbus Statement on Cyber Incident". 30. Januar, 2019. Airbus. https://www.airbus.com/newsroom/press-releases/en/2019/01/airbus-statement-on-cyber-incident.html

35. "Airbus data breach impacts employees in Europe" 30. Januar, 2019. ZDNet. https://www.zdnet.com/article/airbus-data-breach-impacts-employees-in-europe/

36. "Massive Quest Diagnostics data breach impacts 12 million patients". 4. Juni, 2019. ZDNet. https://www.zdnet.com/article/massive-quest-diagnostics-data-breach-impacts-12-million-patients/

37. "Hackers crack 15M LifeLabs accounts, obtain lab results and health card numbers". 17. Dezember, 2019. Daily Hive. https://dailyhive.com/calgary/lifelabs-hacked-cyber-attack

38. "Why the LifeLabs Hack Likely Is Worse than Most". 18. Dezember, 2019. The Tyee. https://thetyee.ca/Analysis/2019/12/18/LifeLabs-Data-Hack/

39. "Personal Information in City of Pensacola Cyberattack". 17. Januar, 2020. City of Pensacola. https://www.cityofpensacola.com/CivicSend/ViewMessage/Message/100944

40. "Personal data of 2,400 Mindef, SAF staff may have been leaked" 22. Dezember, 2019. The Straits Times - Singapore. https://www.straitstimes.com/singapore/personal-data-of-2400-mindef-saf-staff-may-have-been-leaked

Literaturangaben

41. AVTEST – The Independent IT-Security Institute. https://www.av-test.org/en/

42. "Real world protection tests." AV Comparatives. https://www.av-comparatives.org/dynamic-tests/

43. "The ThreatHunting Project." https://www.threathunting.net/data-index

44. Mark Russinovich, Thomas Garnier. "Sysmon v11.10." 24. Juni, 2020. Microsoft. https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

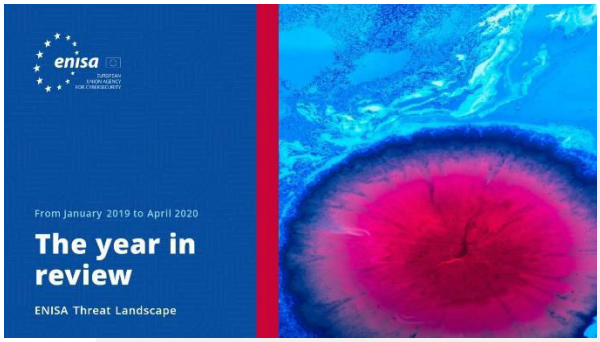
45. "Guide to Intrusion Detection and Prevention Systems (IDPS)." Februar 2007 CSRC. https://csrc.nist.gov/publications/detail/sp/800-94/final

47. "Most malware in Q1 2020 was delivered via encrypted HTTPS connections". 25. Juni 2020. Help Net Security. https://www.helpnetsecurity.com/2020/06/25/encrypted-malware/

48. "Malware statistics and facts for 2020" 29. Juli, 2020. Comparitech. https://www.comparitech.com/antivirus/malware-statistics-facts/


„Die Bedrohungslage wird immer schwieriger greifbar. Nicht nur Angreifer entwickeln neue Techniken, um Sicherheitssysteme zu umgehen, sondern Bedrohungen werden bei gezielten Angriffen immer komplexer und präziser. “
In ETL 2020

Themenbezogen



ENISA Threat Landscape Bericht **Das Berichtsjahr**

Eine Zusammenfassung der Cybersicherheitstrends für den Zeitraum zwischen Januar 2019 und April 2020.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht **Liste der 15 größten Bedrohungen**

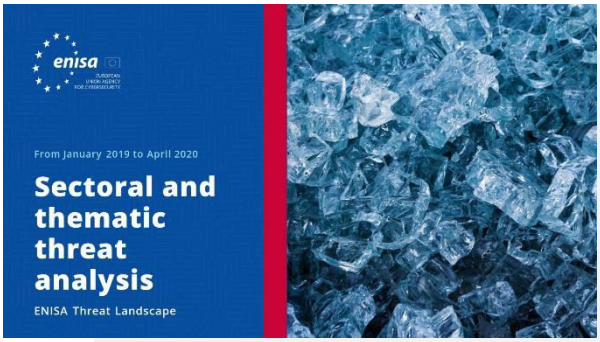
ENISAs-Liste der 15 größten Bedrohungen im Zeitraum zwischen Januar 2019 und April 2020.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht **Forschungsthemen**

Empfehlungen zu Forschungsthemen aus verschiedenen Quadranten der Cybersicherheit und Cyber Threat Intelligence.

LESEN SIE DEN BERICHT



LESEN SIE DEN BERICHT

ENISA Threat Landscape-Bericht
Sektorale und thematische Bedrohungsanalyse

Kontextualisierte Bedrohungsanalyse zwischen Januar 2019 und April 2020.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht
Aufkommende Trends

Die bedeutendsten Cybersicherheitstrends, die zwischen Januar 2019 und April 2020 beobachtet wurden.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht
Übersicht über Cyber Threat Intelligence

Der aktuelle Stand der Cyber Threat Intelligence in der EU.

Über

_ Die Agentur

Die Agentur der Europäischen Union für Cybersicherheit, ENISA, hat die Aufgabe, zu einer hohen Cybersicherheit innerhalb der Union beizutragen. Die Agentur der Europäischen Union für Cybersicherheit wurde 2004 gegründet und durch das EU-Gesetz zur Cybersicherheit gestärkt. Sie trägt zur Unionspolitik im Bereich der Cybersicherheit bei, erhöht die Vertrauenswürdigkeit von ICT-Produkten, -Diensten und -Prozessen durch Programme für die Cybersicherheitszertifizierung, sie kooperiert mit den Mitgliedstaaten und Organen der EU und unterstützt Europa dabei, sich den künftigen Herausforderungen im Bereich der Cybersicherheit zu stellen. Durch Wissensaustausch, Aufbau von Fähigkeiten und Sensibilisierung in Bezug auf Cybersicherheit arbeitet die Agentur gemeinsam mit ihren wichtigsten Interessenträgern darauf hin, das Vertrauen in die vernetzte Wirtschaft zu stärken, die Infrastruktur der Union abwehrfähiger zu machen und schließlich ein sicheres digitales Umfeld für die Gesellschaft und die Bürger Europas zu gewährleisten. Weitere Information über die ENISA und ihre Arbeit finden Sie unter www.enisa.europa.eu.

Mitwirkende

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) und *alle Mitglieder der ENISA CTI Interessenvertreter:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) und Thomas Hemker.

Herausgeber

Marco Barros Lourenço (ENISA) und Louis Marinos (ENISA).

Kontaktangaben

Für Fragen über dieses Dokument, verwenden Sie bitte enisa.threat.information@enisa.europa.eu.

Für Medienanfragen zu dieser Stellungnahme verwenden Sie bitte die folgenden Kontaktangaben: press@enisa.europa.eu.

Wir würden gerne Ihr Feedback zu diesem Bericht erhalten!
Bitte nehmen Sie sich einen Moment Zeit, um den Fragebogen auszufüllen. Um das Formular zu öffnen, können Sie hier klicken.

Impressum/Rechtshinweise

Sofern nichts anderes angegeben ist, gibt diese Veröffentlichung die Ansichten und Auslegungen der ENISA wieder. Diese Veröffentlichung ist nicht als eine Maßnahme der ENISA oder ihrer Gremien auszulegen, sofern sie nicht gemäß der Verordnung (EU) Nr. 526/2013 angenommen wurde. Diese Veröffentlichung entspricht nicht unbedingt dem neuesten Stand und kann in angemessenen Abständen aktualisiert werden.

Quellen von Dritten werden zitiert, sofern erforderlich. Die ENISA haftet nicht für den Inhalt der externen Quellen, einschließlich externer Websites, auf die in dieser Veröffentlichung verwiesen wird.

Die vorliegende Veröffentlichung ist nur für Informationszwecke gedacht. Sie muss kostenlos zugänglich sein. Weder die ENISA noch in deren Namen oder Auftrag tätige Personen können für die Nutzung der in dieser Veröffentlichung enthaltenen Informationen haftbar gemacht werden.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Griechenland
Tel.: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu